



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/909,709	07/20/2001	David Kuehr-McLaren	5577-227	1497

20792 7590 12/16/2004

MYERS BIGEL SIBLEY & SAJOVEC  
PO BOX 37428  
RALEIGH, NC 27627

EXAMINER

PYZOCHA, MICHAEL J

ART UNIT PAPER NUMBER

2137

DATE MAILED: 12/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/909,709	KUEHR-MCLAREN ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Michael Pyzocha	2137	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 20 July 2001.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-46 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-6, 14-16, 20-28, 31-35, 37-42 and 44-46 is/are rejected.
- 7) ☒ Claim(s) 7-13, 17-19, 29, 30, 36 and 43 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 20 July 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                        | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)               | Paper No(s)/Mail Date. _____  |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>07202001</u> .  | 6) <input type="checkbox"/> Other: _____                                    |

Art Unit: 2137

**DETAILED ACTION**

1. Claims 1-46 are pending.

***Claim Rejections - 35 USC § 103***

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-6, 14-16, 20-28, 31-35, 37-42, 44-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gennaro et al ("How to Sign Digital Streams"), in further view of "Introduction to Distributed Memory Programming" (hereinafter CSU) and further in view of Wagner et al ("Analysis of the SSL 3.0 protocol").

As per claims 1, 26, 33, 40, Gennaro et al discloses generating a group MAS based on a data block (see page 4).

Gennaro et al fails to disclose the data block being broken up into packets.

However, CSU discloses breaking data into packets (see page 10 "Moving data between buffers").

Art Unit: 2137

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use CSU's method of breaking data blocks into packets in the authentication method of Gennaro et al.

Motivation to do so would have been to split the data into smaller segments to deal with different capacities (see CSU page 10).

The modified Gennaro et al and CSU system fails to disclose transmitting the packets with a MAC over a SSL connection.

However, Wagner et al discloses the use of an SSL based connection to transmit data (see page 1).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Wagner et al's method of sending data over a SSL connection to send the modified Gennaro et al and CSU's data.

As per claims 2, 27, 34, 41, the modified Gennaro et al, CSU, and Wagner et al system discloses transmitting a record count using the SSL-based protocol connection, the record count indicating a number of data records to be received associated with a next group MAC to be received, the data records associated with the record count corresponding to a next plurality of communication packets to be transmitted and wherein the next group MAC is generated based on the next plurality of

Art Unit: 2137

communication packets to be transmitted (see Gennaro et al page 3 bottom of paragraph 3).

As per claims 3, 35, 42, the modified Gennaro et al, CSU, and Wagner et al system discloses the record count is transmitted using the SSL-based protocol connection before the next plurality of communication packets and wherein the next group MAC is transmitted after the next plurality of communication packets (see Gennaro et al page 3 and page 4).

As per claim 4, the modified Gennaro et al, CSU, and Wagner et al system discloses the record count is transmitted using the SSL-based protocol connection either with the first plurality of communication packets or at a beginning of the next plurality of communication packets (see Gennaro et al page 3).

As per claim 5, the modified Gennaro et al, CSU, and Wagner et al system discloses the record count is transmitted following the generated group MAC without any intervening data records (see Gennaro et al page 3 and page 4).

As per claims 6, 28, the modified Gennaro et al, CSU, and Wagner et al system discloses transmitting a last plurality of communication packets using the SSL-based protocol connection along with a last group MAC, the last group MAC being generated based on the last plurality of communication packets; and closing the SSL-based protocol connection following transmission

Art Unit: 2137

of the last plurality of communication packets (see Gennaro et al page 4 where it is inherent the connection is closed after the transmission of the last set of data).

As per claims 14-16, 20-25, 31-32, 37-39, 44-46, the modified Gennaro et al, CSU, and Wagner et al system discloses the receiving and checking of the group MACs, record counts, and data packets (see Gennaro et al page 3-4, Wagner et al section 4.9 where it is inherent that a fatal alert will terminate the connection) being sent in the above rejected claims.

#### ***Allowable Subject Matter***

4. Claims 7-13, 17-19, 29-30, 36, 43 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

#### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

Art Unit: 2137

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

*Andrew Caldwell*  
Andrew Caldwell